Listing of Claims

1. (Currently Amended) A system for identifying an individual over a communication network; comprising:

a User that needs to be identified in e-commerce;

a Central-Entity that provides digital identity to the Users to positively identify themselves in e-commerce;

an External-Entity offering goods or services and needs to authenticate the Users in e-commerce based on User's digital identity;

a communication network for the User, the Central-Entity and the External-Entity to send and receive information between each other;

whereby the External-Entity ~~may~~ forwards digital identity received from a User to the Central-Entity for authentication; and

wherein the User does not require use of software received from the Central-Entity or a personal identity card to employ digital identity.

2. (Previously Presented) The system according to claim 1, wherein said digital identity includes SecureCode and other information such as UserName.

3. (Previously Presented) The system according to claim 2, wherein said SecureCode is a dynamic, non-predictable and time dependent alphanumeric code, secret code, PIN or other code.

4. (Original) The system according to claim 1, wherein said communication network includes Internet, wireless and private networks.

5. (Previously Presented) A method for identifying an individual; comprising the steps:

The user registers at the Central-Entity;

The user provides his personal and/or financial information to the Central-Entity;

The user receives his unique UserName and Password from the Central-Entity;

The user attempts to get access to a restricted web site or to buy goods and/or services from an External-Entity;

The External-Entity requests the user to authenticate himself using his digital identity;

The user requests SecureCode from the Central-Entity;

The Central-Entity generates dynamic, non-predictable and time dependable SecureCode for the user;

The Central-Entity stores a copy of the SecureCode and sends out the SecureCode to the user over a communication network;

The user receives the SecureCode over a communication network;

The user submits his SecureCode as part of the digital identity in response to External-Entity's request;

The External-Entity forwards the user's digital identity along with the identification and authentication request to the Central-Entity over a communication network;

The Central-Entity retrieves the user's digital identity including the SecureCode from the System;

The Central-Entity compares the retrieved user's digital identity with the digital identity received from the External-Entity;

The Central-Entity sends approval identification and authorization message to the External-Entity when the digital identity forwarded to the Central-Entity, matches the user's digital identity retrieved from the system;

The Central-Entity sends a denial identification and authorization message to the External-Entity when the digital identity forwarded to the Central-Entity does not match the user's digital identity retrieved from the system; and

wherein the user is not required to use software received from the Central-Entity to employ the digital identity.

6. (Previously Presented) The system according to claim 1, wherein the Central Entity corresponds to a Bank or other financial institution, and the User receives the digital identity from the Bank or other financial institution.

7. (Previously Presented) The method of claim 5, wherein the Central Entity corresponds to a Bank or other financial institution, and the User receives the digital identity from the Bank or other financial institution.